Notice of Allowability	Application No. 09/463,907	Applicant(s) MORIAI ET AL.
	Examiner Christian La Forgia	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/11/06*.
2. ☒ The allowed claim(s) is/are *6,13-16,18-23,25,26,31 and 32*.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 2/2/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *mailed with* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Larry Hume (Reg. No. 44,163) on 23 October 2006.

The application has been amended as follows:

6. (Currently Amended) A random function generating apparatus for a data encryption device comprising:

input means for inputting digital signals representing parameter values of each of a plurality of functions each of a composite function composed of first and second functions of different algebraic structures, and for storing them in storage means;

candidate function generating means for generating candidate functions each of said composite function formed of said first and second functions of different algebraic structures based on said plurality of parameters read out of the storage means;

resistance evaluating means for evaluating the resistance of each of said candidate functions to a cryptanalysis; and

selecting means for selecting those of said resistance-evaluated candidate functions which are highly resistant to said cryptanalysis and outputting digital signals representing selected ones of said resistance-evaluated candidate functions;

wherein one of said first and second functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis,

wherein said input means is adapted to input digital signals representing input difference values Δx and output mask values Γy and storing them in the storage means, and said resistance evaluating means comprises at least one of:

higher-order-differential cryptanalysis resistance evaluating means for: calculating a minimum value of the degree of a Boolean polynomial for input bits by which output bits of each of said candidate functions are expressed; and evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation;

interpolation-cryptanalysis resistance evaluating means for: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; and evaluating the resistance of said each candidate function to interpolation cryptanalysis based on the result of said number;

partitioning-cryptanalysis resistance evaluating means for: dividing all input values of the function to be evaluated and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationships between the input subset and the output subset with respect to their average corresponding relationship; and evaluating the resistance of said candidate function to partitioning cryptanalysis based on the result of said calculation; and

differential-linear cryptanalysis resistance evaluating means for: calculating, for every set of input difference value Δx and output mask value Γy of the function S(x) to be evaluated, a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1; and evaluating the resistance of said candidate function to differential-linear cryptanalysis based on the result of said calculation.

Claim 8. (Cancelled)

Allowable Subject Matter

Claims 6, 13-16, 18-23, 25, 26, 31, and 32 are allowed.

The reasons for allowance are clear in light of the Examiner's amendment above and the Applicant's arguments filed with the Appeal Brief of 11 August 2006.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia

Patent Examiner
Art Unit 2131
clf

CHRISTOPHER REVAK
PRIMARY EXAMINER